Blockchain Frontier Technology (B-Front)
Vol. 6, No. 2, January, 2027, pp. 156∼167
E-ISSN: 2808-0009 | P-ISSN: 2808-0831, DOI: 10.34306

A Literature Review of Smart Contract Performance Across Blockchain Environments

Dwi Cahyono[1*], Shofiyul Millah[2], Franses Gabriela Barasa[3], Yasir Mustafa Kareem[4]
[1]Faculty of Economics and Business, University of Muhammadiyah Jember, Indonesia
[2]Faculty of Economics and Business, Universitas Raharja, Indonesia
[3]Faculty of Science and Technology, Universitas Raharja, Indonesia
[4]Department of Technology, Eesp Incorporation, Colombia
[1]dwicahyono@unmuhjember.ac.id, [2]shofiyul@raharja.info, [3]franses@raharja.info, [4]mustafa.kar33m@eesp.io
***Corresponding Author**

Article Info

Article history:

Submission, 22-06-2026
Revised, 18-08-2026
Accepted, 27-08-2026
Published, 31-08-2026

Keywords:

Smart Contract
Performance
Interoperability
Blockchain
Governance

ABSTRACT

Smart contracts have become an important component of blockchain ecosystems because they enable automated, transparent, and decentralized digital processes. However, their performance varies across blockchain environments due to differences in architecture, consensus mechanisms, transaction costs, scalability, security, governance, and interoperability. Existing studies often examine isolated performance indicators or individual blockchain platforms, limiting comprehensive cross-platform understanding. **This study aims** to comparatively analyze smart contract performance across major blockchain platforms, identify technical and contextual factors influencing performance, and synthesize emerging research trends and future research opportunities. **A Structured Literature Review** was conducted using literature obtained from Scopus, IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, and Google Scholar. Peer-reviewed English publications from 2020–2026 were selected through a PRISMA-based screening process. The reviewed studies were systematically analyzed based on blockchain platforms, application domains, performance metrics, security, governance, scalability, and interoperability. **The review identifies Ethereum**, BNB Chain, Solana, Polygon, Hyperledger Fabric, and Avalanche as major platforms with distinct performance characteristics and trade-offs. Throughput, latency, transaction cost, and scalability are prominent technical dimensions, while security, governance, and interoperability provide essential contextual perspectives. The findings indicate that no single platform consistently provides superior performance across all application requirements. **Smart contract** performance should be evaluated using a multidimensional approach rather than a single technical indicator. Future research should emphasize interoperability, Layer-2 scalability, cross-chain smart contracts, security assurance, and governance to support more comprehensive blockchain performance evaluation.

DOI: https://doi.org/10.34306/b-front.v6i2.1176

1. INTRODUCTION

Blockchain technology enables decentralized, transparent, and tamper-resistant data management across various sectors, including finance, supply chain management, healthcare, education, and public services

[1, 2]. At the core of this technology are smart contracts, which automatically execute predefined agreements without requiring intermediaries, thereby improving operational efficiency, reducing transaction costs, and enhancing trust among participating entities [3]. As organizations continue to accelerate digital transformation, smart contracts have become essential components for automating business processes and supporting secure digital ecosystems [4]. Their growing adoption also contributes to sustainable digital innovation, particularly by supporting Sustainable Development Goal (SDG) 9 through resilient digital infrastructure and SDG 16 by promoting transparency, accountability, and trustworthy digital transactions.

Despite their increasing adoption, the implementation of smart contracts continues to face significant technical and operational challenges. Performance varies considerably across blockchain platforms due to differences in consensus mechanisms, network architectures, execution environments, transaction costs, scalability, and security models. These variations directly affect critical performance indicators such as throughput, latency, execution efficiency, and resource consumption. Although numerous studies have evaluated smart contract performance, most investigations focus on individual blockchain platforms or emphasize isolated performance aspects without providing comprehensive cross-platform comparisons. Consequently, stakeholders often lack a holistic understanding of the relative strengths and limitations of different blockchain ecosystems when selecting suitable platforms for specific applications.

Existing review and empirical studies generally examine smart contract performance from limited perspectives, such as transaction efficiency, consensus algorithms, security vulnerabilities, or scalability [5, 6]. While these studies provide valuable insights, they rarely integrate multiple performance dimensions into a unified analytical perspective [7]. Furthermore, recent developments involving Layer-2 scaling solutions, blockchain interoperability, governance mechanisms, and application-specific implementations have received limited attention within comparative review studies [8]. As a result, a comprehensive literature synthesis that systematically compares blockchain platforms based on measurable performance metrics, security characteristics, governance mechanisms, and application domains remains insufficiently explored [9]. This gap limits the ability of researchers and practitioners to understand the evolving landscape of smart contract performance comprehensively.

To address these limitations, this study presents a structured comparative literature review that synthesizes findings from recent research on smart contract performance across multiple blockchain environments. Unlike previous review studies, this research develops a comparative evaluation framework that integrates key performance indicators, including throughput, latency, transaction cost, scalability, security, governance, and interoperability. In addition, the reviewed studies are categorized according to their application domains, allowing a broader understanding of smart contract adoption across different industries. The study also identifies emerging research trends and highlights current challenges and future opportunities associated with blockchain performance optimization, thereby providing a more comprehensive perspective than existing literature reviews.

The study therefore aims to systematically review and compare smart contract performance across blockchain environments, identify the key factors affecting performance, and develop an integrated evaluation framework that considers technical, security, and governance dimensions. To systematically address the identified research gap, this study formulates the following research questions:

- RQ1: How does smart contract performance vary across different blockchain environments?
- RQ2: What technical, security, and governance factors influence smart contract performance across blockchain environments?
- RQ3: How can the identified performance factors be integrated into a comprehensive framework for evaluating smart contract performance across blockchain environments?

Based on the identified research gaps, this study aims to conduct a comprehensive comparative analysis of smart contract performance across various blockchain platforms through a SLR approach. Specifically, the study seeks to compare the performance characteristics of major blockchain ecosystems, identify the technical factors influencing smart contract performance, analyze security and governance considerations, classify blockchain applications across different domains, synthesize recent research trends, and propose future research directions related to interoperability, Layer-2 scaling technologies, and cross-chain smart contract development.

The findings are expected to provide practical guidance for researchers, developers, and organizations in selecting and optimizing blockchain platforms while contributing to the advancement of blockchain-based digital transformation.

2. LITERATURE REVIEW

2.1. Blockchain Technology and Smart Contracts

Blockchain is a decentralized Distributed Ledger Technology (DLT) that enables secure, transparent, and immutable recording of digital transactions without requiring a centralized authority [10, 11, 12]. Transactions are validated through consensus mechanisms and permanently stored in cryptographically linked blocks, ensuring data integrity and resistance to tampering [13]. These characteristics have driven blockchain adoption across numerous sectors, including finance, healthcare, supply chain management, education, and public administration. One of the most significant innovations enabled by blockchain is the smart contract, which is a self-executing software program that automatically performs predefined actions when specified conditions are satisfied [14, 15]. Unlike conventional digital agreements, smart contracts eliminate intermediary involvement, reduce operational costs, increase transaction speed, and improve trust among participating entities. Their deterministic execution and transparent verification make them fundamental components of Decentralized Applications (DApps) and blockchain-based digital ecosystems [16]. As organizations continue accelerating digital transformation, smart contracts have become increasingly important for automating business processes while improving efficiency, accountability, and transparency across distributed environments [17].

2.2. Smart Contract Performance Metrics

The performance of smart contracts is commonly evaluated using multiple technical indicators that reflect the operational capability of blockchain platforms [18]. Throughput represents the number of transactions processed within a given period, indicating the processing capacity of the network. Latency measures the time required for a transaction to be confirmed and finalized, directly influencing user experience and application responsiveness. Gas fees describe the computational costs required to execute smart contracts, affecting the economic feasibility of blockchain applications [19]. Additional metrics include transaction finality, which determines when transactions become irreversible, scalability, referring to the network's ability to maintain performance as transaction volumes increase, and resource consumption, including computational, storage, and energy requirements during contract execution [20, 21]. Since blockchain platforms adopt different consensus algorithms and execution architectures, significant variations exist in these performance metrics. Therefore, evaluating smart contract performance requires a multidimensional perspective rather than relying on a single indicator [22, 23]. These performance metrics serve as the primary evaluation criteria for the comparative analysis conducted in this study.

2.3. Blockchain Security and Governance

Security and governance are fundamental to the reliability and sustainability of blockchain systems [24]. Smart contracts remain vulnerable to attacks such as reentrancy, oracle manipulation, improper access control, and flash loan attacks, highlighting the importance of secure coding, auditing, and formal verification [25, 26, 27]. Blockchain governance regulates protocol updates, network rules, and stakeholder decisions through on-chain and off-chain mechanisms, including Decentralized Autonomous Organizati (DAOs) [28, 29, 30]. Together, security and governance influence blockchain performance, trustworthiness, and ecosystem sustainability. Therefore, evaluating smart contract performance requires consideration of not only technical efficiency but also the security and governance conditions that shape the reliability of blockchain environments. These dimensions are particularly important because performance improvements that compromise security or governance may reduce overall system reliability and long-term adoption.

2.4. Blockchain Scalability and Interoperability

As blockchain adoption continues to expand, scalability and interoperability have become major challenges for supporting large-scale decentralized applications [31, 32]. Scalability refers to a blockchain network's ability to process increasing transaction volumes while maintaining acceptable throughput, latency, and transaction costs. However, blockchain systems often encounter the Blockchain Trilemma, which suggests that achieving security, decentralization, and scalability simultaneously remains difficult [33, 34]. In parallel, blockchain interoperability enables communication and asset exchange among heterogeneous blockchain networks through cross-chain communication protocols, blockchain bridges, and interoperability frameworks [35]. These technologies reduce ecosystem fragmentation, facilitate collaborative decentralized applications, and improve overall blockchain efficiency [36]. Consequently, scalability and interoperability have become essential considerations in evaluating the performance and future development of smart contract platforms [37].

2.5. Smart Contract Application Domains

The adoption of smart contracts has expanded significantly beyond cryptocurrency transactions into various industrial sectors requiring secure, transparent, and automated digital processes [38, 39]. In the financial sector, smart contracts support Decentralized Finance (DeFi) applications, including digital payments, lending, decentralized exchanges, and asset tokenization [40, 41]. Supply chain systems utilize smart contracts to improve product traceability, logistics management, and inventory verification. Healthcare organizations employ blockchain technology for secure electronic medical records, patient consent management, and pharmaceutical traceability. Within the education sector, smart contracts facilitate academic certificate issuance and credential verification, reducing document forgery and improving verification efficiency. Government institutions also implement smart contracts for digital identity management, electronic voting, and public record administration. These diverse application domains demonstrate that smart contract implementation requires different performance, security, governance, and scalability characteristics depending on the operational context. Therefore, understanding these application domains is essential for selecting appropriate blockchain platforms and designing effective decentralized systems.

Table 1. Major Smart Contract Application Domains

Domain	**Smart Contract Usage**
Finance	Decentralized Finance (DeFi), digital payments, lending, asset tokenization
Supply Chain	Product traceability, logistics automation, inventory verification
Healthcare	Electronic medical records, patient consent management, pharmaceutical traceability
Education	Academic certificate issuance, credential verification, diploma authentication
Government	Digital identity management, electronic voting, public record management

As presented in Table 1, smart contracts are applied across finance, supply chain, healthcare, education, and government, addressing sector-specific needs such as transaction automation, traceability, data security, credential verification, and digital identity. These diverse applications require different levels of performance, security, scalability, and governance, highlighting the need for comparative analysis of blockchain platforms to identify suitable solutions for specific application requirements.

3. RESEARCH METHODOLOGY

3.1. Research Design

This study employed a Structured Literature Review (SLR) to systematically analyze and compare the performance of smart contracts across various blockchain platforms [42]. Unlike conventional narrative reviews, a SLR follows predefined procedures for identifying, selecting, evaluating, and synthesizing relevant studies, thereby improving transparency and reproducibility. The review focuses on comparative analyses of blockchain platforms by examining their performance characteristics, security mechanisms, governance models, scalability, interoperability, and application domains. Through this approach, the study aims to provide a comprehensive understanding of the factors influencing smart contract performance while identifying current research trends and future research opportunities [43, 44].

3.2. Literature Search Strategy

Relevant literature was collected from Scopus, IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, and Google Scholar using keywords related to smart contracts, blockchain, performance, scalability, security, interoperability, governance, and Layer-2. Peer-reviewed English publications from 2020–2026 were included, while duplicates, non-peer-reviewed, inaccessible, and irrelevant studies were excluded. The selection process followed PRISMA-based screening to ensure relevant and high-quality studies were included. The selected studies were then systematically analyzed and synthesized based on blockchain platform, performance characteristics, security considerations, governance mechanisms, and application contexts. Data were extracted using predefined categories to maintain consistency across the reviewed studies. The extracted information included blockchain platforms, smart contract characteristics, performance indicators, security issues, governance mechanisms, and application domains. Comparative analysis was subsequently conducted to identify common patterns, differences, research gaps, and factors influencing smart contract performance across different blockchain environments.

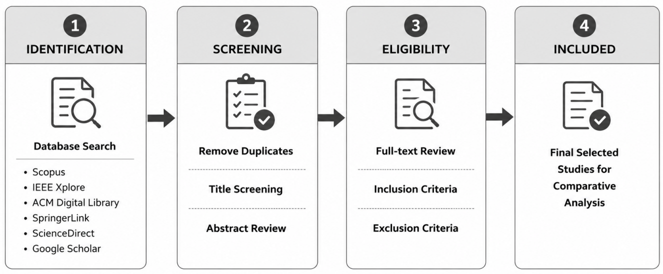

Figure 1. PRISMA-Based Literature Selection Process

Figure 1 illustrates the structured literature selection process adopted in this study based on the PRISMA guidelines. The process consists of four main stages: identification, screening, eligibility assessment, and final inclusion of relevant studies. This systematic procedure enhances the transparency, consistency, and reproducibility of the literature review while minimizing potential selection bias.

3.3. Data Extraction and Comparative Analysis

Information from the selected studies was systematically extracted and organized to facilitate comparative analysis across blockchain platforms. The extracted information included publication details, blockchain platform, application domain, performance metrics, security aspects, governance mechanisms, interoperability support, scalability approaches, and the major findings reported by each study. The extracted data were subsequently synthesized to identify similarities, differences, strengths, limitations, and emerging research trends among blockchain ecosystems.

Table 2. Data Extraction Framework

Study	Blockchain Platform	Application Domain	Performance Metrics	Key Findings
[45]	Ethereum, Solana	General Blockchain	Throughput, Latency, Scalability	Compared architectural differences between Ethereum and Solana, highlighting trade-offs between decentralization and transaction performance
[46]	Ethereum, Solana, Cardano, Algorand, Aptos, Tezos	Smart Contract Development	Security, Usability, Programming Features	Proposed a benchmark for evaluating smart contract languages across major blockchain ecosystems
[39]	Ethereum, BNB Chain, Avalanche, Polygon	Vehicle-to-Everything (V2X), Internet of Things (IoT), smart transportation	Gas fees, throughput	The study compares transaction gas fees across Ethereum, BNB Chain, Avalanche, and Polygon and evaluates blockchain throughput for (Vehicle-to-Blockchain) V2B applications
[47]	Hyperledger Fabric, Private Ethereum	Enterprise Applications	Throughput, Latency, Scalability	Hyperledger Fabric significantly outperformed private Ethereum in transaction throughput and execution latency under enterprise workloads
[48]	Solana, with Ethereum used as comparison context	Smart-contract security	Vulnerability prevalence, developer security, code-review performance	The study investigates security challenges in Solana smart-contract development and reports that deployed-contract vulnerability prevalence was below 0.3% for the vulnerabilities examined, despite substantial developer difficulties in identifying vulnerabilities
[49]	Ethereum	Smart-contract ecosystem / security	Contract dependencies, interaction volume, deployer concentration, dependency risks	The study analyzes more than 41 million Ethereum contracts and 11 billion interactions, identifying substantial dependency and centralization risks in the smart-contract ecosystem

As shown in Table 2, each selected study was systematically categorized according to its blockchain platform, application domain, evaluation metrics, and principal findings. This structured extraction process facilitates a systematic and comprehensive comparison across the reviewed literature, allowing the identification of similarities, differences, performance characteristics, and research findings across various blockchain environments.

3.4. Proposed Smart Contract Performance Evaluation Framework

To provide a more comprehensive synthesis of previous studies, this research proposes a Smart Contract Performance Evaluation Framework that integrates multiple evaluation dimensions affecting blockchain performance. Rather than assessing blockchain platforms solely based on technical performance indicators, the framework incorporates security, governance, scalability, interoperability, and application perspectives into a unified analytical model. This multidimensional framework enables systematic comparisons among blockchain ecosystems while supporting the identification of research trends, practical implications, and future research opportunities.

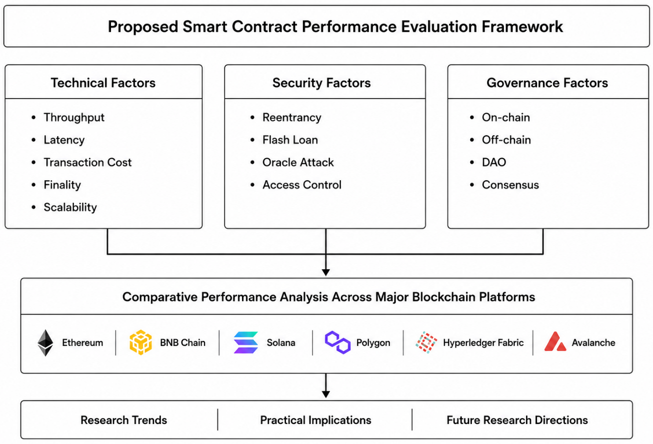

Figure 2. Proposed Smart Contract Performance Evaluation Framework

As illustrated in Figure 2, the proposed evaluation framework integrates three major analytical dimensions technical performance, security, and governance to support a comprehensive comparison of smart contract implementations across multiple blockchain platforms. By combining these dimensions within a unified framework, the study provides a more systematic basis for evaluating blockchain performance than conventional literature reviews that typically emphasize only isolated performance indicators. The framework also serves as the foundation for identifying research trends, practical implications, and future research directions discussed in the subsequent section.

4. RESULTS AND DISCUSSION

4.1. Overview of the Reviewed Literature

The reviewed literature demonstrates increasing interest in evaluating blockchain platforms according to performance, scalability, transaction cost, security, and application requirements. Across the selected studies, six major platforms relevant to this review were identified: Ethereum, BNB Chain, Solana, Polygon, Hyperledger Fabric, and Avalanche. The literature shows that these platforms are investigated in different contexts, ranging from decentralized applications and smart-contract execution to enterprise systems and IoT-based applications. These variations indicate that platform performance cannot be interpreted independently from its intended application context, as different environments prioritize different combinations of efficiency, scalability, security, interoperability, and governance. Consequently, comparative evaluation should consider both technical characteristics and operational requirements to provide a more meaningful assessment of smart-contract performance across blockchain platforms.

The reviewed studies also demonstrate that blockchain performance cannot be evaluated using a single indicator. Throughput and latency are frequently used to assess transaction-processing capability, while transaction cost, scalability, interoperability, and smart-contract execution provide additional perspectives. For example, [39] compared Ethereum, BNB Chain, Avalanche, and Polygon in a V2X and IoT context, while [47] examined Hyperledger Fabric and private Ethereum using throughput, latency, and scalability. These comparisons highlight the importance of considering multiple performance dimensions when evaluating blockchain platforms for different applications.

Table 3. Comparative Findings Across Reviewed Blockchain Platforms

Blockchain Platform	**Performance Characteristics**	**Main Metrics**	**Application Context**	**Identified Trade-offs**
Ethereum	Mature smart-contract ecosystem with comparatively higher transaction overhead in some workloads	Throughput, latency, transaction cost, scalability	DeFi, DApps, enterprise applications	Ecosystem maturity vs. transaction cost and latency
BNB Chain	Competitive transaction performance with relatively lower transaction costs in evaluated applications	Throughput, gas fees	DApps, V2X/IoT	Lower cost vs. decentralization and ecosystem characteristics
Solana	High-performance architecture and strong scalability characteristics	Throughput, scalability, performance	DApps, high-throughput applications	Performance vs. different development and ecosystem model
Polygon	Scalable and relatively cost-efficient environment for DApps	Throughput, gas fees, scalability	DApps, V2X/IoT	Cost efficiency vs. dependence on scaling architecture
Hyperledger Fabric	Strong performance for permissioned enterprise workloads	Throughput, latency, scalability	Enterprise and financial applications	Enterprise performance vs. permissioned architecture
Avalanche	Competitive performance and transaction-cost characteristics	Throughput, gas fees, performance	V2X/IoT, DApps	Performance and cost vs. ecosystem maturity

As shown in Table 3, the reviewed platforms exhibit different performance characteristics and trade-offs. Ethereum provides a mature smart-contract ecosystem, whereas BNB Chain, Polygon, and Avalanche demonstrate competitive cost and performance characteristics in specific application contexts. Solana is associated with high-performance and scalability-oriented architectures, while Hyperledger Fabric is particularly suitable for permissioned enterprise environments. These differences indicate that blockchain platform selection should consider application requirements rather than rely on a single performance indicator.

4.2. Comparative Performance Analysis

The comparative analysis indicates that throughput, latency, transaction cost, and scalability are the most prominent technical dimensions across the reviewed studies. However, direct numerical comparison between platforms should be interpreted cautiously because the studies employ different hardware configurations, workloads, consensus mechanisms, transaction types, and experimental environments.

The comparison between Hyperledger Fabric and private Ethereum provides particularly clear evidence of this trade-off [47] reported that Hyperledger Fabric achieved substantially higher throughput and lower latency for smart-contract invocation, whereas private Ethereum performed better for query operations. Similarly, comparative evaluation in the V2X/IoT context demonstrated that Ethereum, BNB Chain, Avalanche, and Polygon differ in transaction costs and throughput, confirming that platform performance is strongly influenced by application requirements.

Therefore, the findings suggest that high throughput alone does not necessarily indicate superior smart-contract performance. A platform with high transaction-processing capability may still present limitations in transaction cost, interoperability, security, or governance. This supports the multidimensional evaluation approach proposed in this study, in which technical, security, and governance factors are considered together.

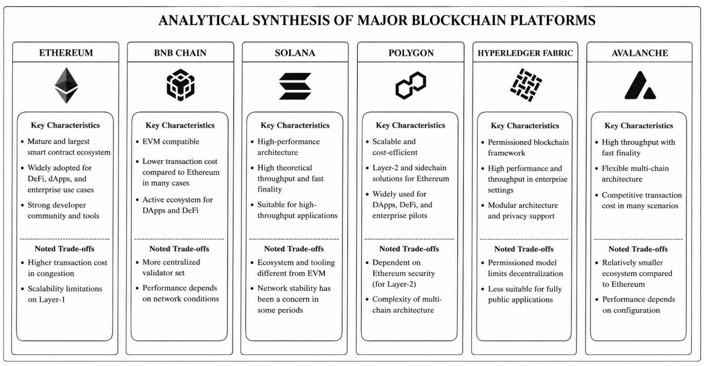

Figure 3. Analytical synthesis of major blockchain platform characteristics and performance trade-offs

Figure 3 presents an analytical comparison of six major blockchain platforms, namely Ethereum, BNB Chain, Solana, Polygon, Hyperledger Fabric, and Avalanche. The comparison highlights their key characteristics, including smart contract capabilities, transaction performance, scalability, interoperability, and enterprise suitability. It also identifies the main trade-offs associated with each platform, such as scalability limitations, network centralization, ecosystem differences, and configuration dependencies. This synthesis provides a basis for understanding the strengths and limitations of each platform when considering blockchain implementation for different application requirements.

4.3. Security, Governance, and Emerging Research Trends

Beyond technical performance, the reviewed literature indicates that security and governance are critical dimensions of smart-contract effectiveness. Smart contracts operate through programmable rules, meaning that vulnerabilities in contract logic, access control, external data dependencies, and contract interactions can affect both system security and operational reliability. Consequently, evaluating smart-contract platforms solely through throughput and latency may provide an incomplete representation of their practical suitability.

Security considerations are particularly important because different blockchain ecosystems employ different execution environments, programming models, and network architectures. These differences can influence the types of vulnerabilities that may occur and the mechanisms available for detecting or mitigating them. Therefore, the comparative framework in this study incorporates security factors alongside technical performance rather than treating security as an independent secondary issue. This integrated perspective enables a more comprehensive assessment of platform suitability across different application contexts.

Governance also represents an important distinction between blockchain ecosystems. Public platforms generally rely on combinations of on-chain mechanisms, community participation, validators, and off-chain decision-making, whereas permissioned platforms such as Hyperledger Fabric provide greater organizational control. This distinction creates a trade-off between decentralization, institutional control, upgrade mechanisms, and accountability. Therefore, governance mechanisms should be considered when evaluating blockchain platforms because they can influence how effectively networks adapt to changing requirements while maintaining transparency and accountability.

The reviewed literature further indicates several emerging research directions. Interoperability, cross-chain smart contracts, Layer-2 scalability, security assurance, and governance mechanisms remain important areas for future research. In particular, increasing interaction between different blockchain ecosystems requires reliable cross-chain communication mechanisms while maintaining security and reducing transaction overhead. Layer-2 solutions also provide an important direction for improving scalability without completely abandoning established Layer-1 ecosystems. Additionally, further research is needed to evaluate their effectiveness across different blockchain environments. Future studies should examine how interoperability and Layer-2 technologies can be integrated without compromising security and governance.

Overall, the findings demonstrate that future smart-contract research should move beyond isolated platform benchmarking toward multidimensional and cross-platform evaluation. Such an approach should simultaneously consider performance, security, governance, interoperability, and application requirements. This synthesis directly supports the proposed evaluation framework and provides a basis for developing more comprehensive blockchain performance benchmarks. Future studies should also consider differences in application contexts, workload characteristics, and blockchain architectures when comparing platform performance. In addition, greater attention should be given to the interaction between technical performance, security, governance, and interoperability rather than evaluating these dimensions independently.

4.4. Implications of the Findings

The findings have important implications for the evaluation and selection of blockchain environments for smart-contract deployment. The observed differences across platforms indicate that performance advantages are highly dependent on application context, workload characteristics, and operational requirements. Consequently, a blockchain environment that performs well under one application scenario may not provide the same advantages under another. This suggests that platform evaluation should move beyond direct comparison of benchmark values and consider the specific requirements and constraints of each deployment context. Such an approach can support more informed platform selection by balancing performance objectives with practical considerations, particularly when smart-contra

The findings also imply that improving one performance dimension may involve trade-offs with other system requirements. Higher transaction throughput, for instance, does not necessarily guarantee lower costs, stronger security, greater interoperability, or more effective governance. Therefore, practitioners and researchers should evaluate these factors collectively when selecting blockchain environments for smart-contract applications. Such evaluation should also consider the characteristics of the intended workload, transaction patterns, scalability requirements, and operational constraints of the deployment environment. A platform that demonstrates superior performance under controlled benchmark conditions may not necessarily provide the same advantages in real-world applications with different usage patterns and resource limitations. This perspective strengthens the practical relevance of the review by providing a basis for more context-aware evaluation and reducing the risk of selecting platforms solely on the basis of isolated performance indicators.

5. MANAGERIAL IMPLICATION

The findings provide practical implications for organizations and decision-makers when selecting blockchain platforms for smart contract implementation. Platform selection should not be based solely on transaction throughput or latency, but should consider multiple factors, including transaction costs, scalability, security, governance, interoperability, and application requirements. Ethereum may be suitable when ecosystem maturity and broad smart-contract support are prioritized, while Solana, BNB Chain, Polygon, Avalanche, and Hyperledger Fabric may offer advantages for specific performance, cost, scalability, or enterprise requirements.

From a practical perspective, for technology managers and developers, the findings emphasize the importance of matching blockchain architecture with the operational context of the intended application [50]. Public blockchain platforms may provide broader ecosystems and decentralized participation, whereas permissioned platforms such as Hyperledger Fabric can provide greater organizational control for enterprise environments [51]. Managers should therefore evaluate workload characteristics, expected transaction volume, security requirements, governance structures, and interoperability needs before deployment.

The findings emphasize the need for ongoing performance and security evaluation as blockchain systems evolve. Organizations should consider Layer-2 solutions, interoperability, smart contract audits, and governance in their long-term strategies. Blockchain also supports SDG 9 through innovation, SDG 16 through transparency, and SDG 12 by improving efficiency. The multidimensional evaluation approach helps ensure better decision-making by assessing technical, security, scalability, and sustainability aspects, leading to more reliable and impactful blockchain adoption. Organizations should continuously evaluate evolving blockchain technologies, integrating Layer-2 solutions, interoperability, audits, and governance while considering SDG 9, SDG 16, and SDG 12 to support secure, transparent, efficient, and sustainable adoption.

6. CONCLUSION

Based on the systematic review findings, this study conducted a SLR to comparatively analyze smart contract performance across major blockchain platforms. The findings show that Ethereum, BNB Chain, Solana, Polygon, Hyperledger Fabric, and Avalanche exhibit different strengths and trade-offs in throughput, latency, transaction cost, scalability, security, governance, and application suitability. Therefore, smart contract performance should not be assessed using a single technical indicator, but through a multidimensional perspective that considers both technical and contextual factors.

The analysis further demonstrates that blockchain platform selection should be aligned with specific application requirements. Ethereum offers ecosystem maturity, Solana emphasizes high performance and scalability, BNB Chain, Polygon, and Avalanche provide competitive cost and performance characteristics, while Hyperledger Fabric is particularly suitable for permissioned enterprise environments. The proposed evaluation framework integrates technical performance, security, and governance, providing a systematic basis for cross-platform comparison and supporting more informed blockchain implementation decisions.

The findings also highlight the broader contribution of blockchain technology to sustainable digital transformation. Blockchain adoption can support SDG 9 (Industry, Innovation, and Infrastructure) through digital innovation, SDG 16 (Peace, Justice, and Strong Institutions) through greater transparency and accountability, and SDG 12 (Responsible Consumption and Production) by improving efficiency in digital transactions and data management. Future research should further examine interoperability, Layer-2 scalability, cross-chain smart contracts, security assurance, and governance to develop more comprehensive and sustainable blockchain performance benchmarks.

7. DECLARATIONS

7.1. About Authors

Dwi Cahyono (DC) https://orcid.org/0000-0002-2933-0973

Shofiyul Millah (SM) https://orcid.org/0000-0002-6696-9450

Franses Gabriela Barasa (FG) https://orcid.org/0009-0007-1051-5226

Yasir Mustafa Kareem (YM) https://orcid.org/0009-0008-5096-2300

7.2. Author Contributions

Conceptualization: DC ; Methodology: SM ; Software: FG; Validation: YM ; Formal Analysis: DC and SM; Investigation: FG; Resources: YM; Data Curation: SM; Writing Original Draft Preparation: YM and SM; Writing Review and Editing: FG; Visualization: YM; All authors, DC, SM, FG and YM have read and agreed to the published version of the manuscript

7.3. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

7.4. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

7.5. Declaration of Conflicting Interest

The authors declare that they have no conflicts of interest, known competing financial interests, or personal relationships that could have influenced the work reported in this paper.

REFERENCES

[1] C. Gilbert and M. A. Gilbert, "The integration of blockchain technology into database management systems for enhanced security and transparency," *International Research Journal of Advanced Engineering and Science*, vol. 9, no. 4, pp. 316–334, 2024.

[2] N. Kumar, K. Kumar, A. Aeron, and F. Verre, "Blockchain technology in supply chain management: Innovations, applications, and challenges," *Telematics and Informatics Reports*, vol. 18, p. 100204, 2025.

[3] C. Barraza-Botet, D. Nadal, M. Rosen, and D. Winickoff, "A comparison of the innovation and regulatory environments for biotechnology and biosolutions across the european union and the united states," OECD Publishing, Paris, Tech. Rep. 2026/02, 2026. [Online]. Available: https://doi.org/10.1787/1ec20342-en

[4] A. Pambudi, O. Wilson, and J. Zanubiya, "Exploring the synergy of global markets and digital innovation in business growth using smartpls," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 6, no. 1, pp. 106–113, 2024.

[5] U. Rahardja, Q. Aini, A. S. Bist, S. Maulana, and S. Millah, "Examining the interplay of technology readiness and behavioural intentions in health detection safe entry station," *JDM (Jurnal Dinamika Manajemen)*, vol. 15, no. 1, pp. 125–143, 2024.

[6] V. Piantadosi, G. Rosa, D. Placella, S. Scalabrino, and R. Oliveto, "Detecting functional and security-related issues in smart contracts: A systematic literature review," *Software: Practice and experience*, vol. 53, no. 2, pp. 465–495, 2023.

[7] J. B. Hendrawidjaja, B. W. Soetjipto, R. D. Kusumastuti, and O. Jayanagara, "Ecosystem exchange, strategic capabilities, and firm performance with agility and innovation mediators," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 1, pp. 226–238, 2026.

[8] G. Zhu, D. He, H. An, M. Luo, and C. Peng, "The governance technology for blockchain systems: a survey," *Frontiers of Computer Science*, vol. 18, no. 2, p. 182813, 2024.

[9] S. Kosasi, U. Rahardja, I. D. A. E. Yuliani, R. Laipaka, B. Susilo, and H. Kikin, "It governance: Performance assessment of maturity levels of rural banking industry," in *2022 4th International Conference on Cybernetics and Intelligent System (ICORIS)*. IEEE, 2022, pp. 1–6.

[10] S. Dong, K. Abbas, M. Li, and J. Kamruzzaman, "Blockchain technology and application: an overview," *PeerJ Computer Science*, vol. 9, p. e1705, 2023.

[11] R. Fahrudin, Y. F. DWI, F. A. YADI, A. Wilson, and T. Kuusk, "Addressing regulatory risks in fintech through decentralized technologies," *APTISI TRANSACTIONS ON MANAGEMENT: iLearning Journal Center*, vol. 8, no. 3, pp. 204–212, 2024.

[12] A. Sunyaev, "Distributed ledger technology," in *Internet computing: Principles of distributed systems and emerging internet-based technologies*. Springer, 2024, pp. 239–272.

[13] J. I. Senarathna, "The role of cryptography in blockchain: ensuring immutability, transparency and security," 2025.

[14] M. Fiore, A. Capodici, P. Rucci, A. Bianconi, G. Longo, M. Ricci, F. Sanmarchi, and D. Golinelli, "Blockchain for the healthcare supply chain: A systematic literature review," *Applied Sciences*, vol. 13, no. 2, p. 686, 2023.

[15] M. N. Ayubi, S. Anggoro, and Y. M. Kareem, "Decentralized decision intelligence using ai and blockchain in modern enterprises," *ADI Journal on Recent Innovation*, vol. 7, no. 1, pp. 38–49, 2025.

[16] P. Zheng, Z. Jiang, J. Wu, and Z. Zheng, "Blockchain-based decentralized application: A survey," *IEEE Open Journal of the Computer Society*, vol. 4, pp. 121–133, 2023.

[17] X. Ye, N. Zeng, X. Tao, D. Han, and M. König, "Smart contract generation and visualization for construction business process collaboration and automation: Upgraded workflow engine," *Journal of Computing in Civil Engineering*, vol. 38, no. 6, p. 04024030, 2024.

[18] N. S. Shibu, A. R. Devidas, S. Balamurugan, S. Ponnekanti, and M. V. Ramesh, "Optimizing microgrid resilience: integrating iot, blockchain, and smart contracts for power outage management," *IEEE Access*, vol. 12, pp. 18 782–18 803, 2024.

[19] H. Kim and D. Kim, "Optimal gas fee minimization in defi: Enhancing efficiency and security on the ethereum blockchain," *IEEE Access*, vol. 12, pp. 173 810–173 823, 2024.

[20] T. Yu, F. Luo, C. Pu, Z. Zhao, and G. Ranzi, "Dual-blockchain-based p2p energy trading system with an improved optimistic rollup mechanism," *IET Smart Grid*, vol. 5, no. 4, pp. 246–259, 2022.

[21] B. Severin, M. Hesenius, F. Blum, M. Hettmer, and V. Gruhn, "Smart money wasting: Analyzing gas cost drivers of ethereum smart contracts," in *2022 IEEE International Conference on Software Maintenance and Evolution (ICSME)*. IEEE, 2022, pp. 293–304.

[22] M. F. Djamali, D. Lusiana, A. Parastry, and O. A. Al-Kamari, "Optimizing business workflow using ai integrated blockchain platforms," *ADI Journal on Recent Innovation*, vol. 7, no. 1, pp. 62–74, 2025.

[23] M. Touloupou, M. Themistocleous, E. Iosif, and K. Christodoulou, "A systematic literature review toward a blockchain benchmarking framework," *IEEE Access*, vol. 10, pp. 70 630–70 644, 2022.

[24] S. Siddiqui, S. Hameed, S. A. Shah, J. Arshad, Y. Ahmed, and D. Draheim, "A smart-contract-based adaptive security governance architecture for smart city service interoperations," *Sustainable Cities and Society*, vol. 113, p. 105717, 2024.

[25] G. Kabanda, "Advancing resilience in ethereum, bitcoin, and blockchain technology: a comprehensive analysis of scalability, security, and sustainability challenges in a vuca world," *International Journal of Blockchains and Cryptocurrencies*, vol. 6, no. 2, pp. 113–131, 2025.

[26] A. Kristian, A. R. Az-Zahra, F. Hidayat, A. Y. Fauzi, and E. Kallas, "Enhancing cybersecurity risk management strategies in financial institutions: A comprehensive analysis of threats and mitigation approaches," *Journal of Computer Science and Technology Application*, vol. 1, no. 2, pp. 96–103, 2024.

[27] H. Rameder, M. Di Angelo, and G. Salzer, "Review of automated vulnerability analysis of smart contracts on ethereum," *Frontiers in Blockchain*, vol. 5, p. 814977, 2022.

[28] L. Heimbach and R. Wattenhofer, "Sok: Preventing transaction reordering manipulations in decentralized finance," in *Proceedings of the 4th ACM Conference on Advances in Financial Technologies*, 2022, pp. 47–60.

[29] S. Bonnet and F. Teuteberg, "Decentralized autonomous organizations: A systematic literature review and research agenda," *International Journal of Innovation and Technology Management*, vol. 21, no. 04, p. 2450026, 2024.

[30] C. Chambefort and M. Chaudey, "Blockchain, tokens, smart contracts, and "decentralized autonomous organization": Expanding and renewing the mechanisms of governance?" *European Management Review*, vol. 21, no. 3, pp. 511–515, 2024.

[31] M. H. Nasir, J. Arshad, M. M. Khan, M. Fatima, K. Salah, and R. Jayaraman, "Scalable blockchains—a systematic review," *Future generation computer systems*, vol. 126, pp. 136–162, 2022.

[32] A. Rizky, M. Z. Firli, N. A. Lindzani, S. Audiah, L. Pasha *et al.*, "Advanced cyber threat detection: Big

data-driven ai solutions in complex networks," *Journal of Computer Science and Technology Application*, vol. 1, no. 2, pp. 136–143, 2024.

[33] G. Quattrocchi, F. Scaramuzza, and D. A. Tamburri, "The blockchain trilemma: an evaluation framework," *IEEE Software*, vol. 41, no. 6, pp. 101–110, 2024.

[34] S. Reno and M. M. Haque, "Solving blockchain trilemma using off-chain storage protocol," *IET information security*, vol. 17, no. 4, pp. 681–702, 2023.

[35] D. Tortola, A. Lisi, P. Mori, and L. Ricci, "Tethering layer 2 solutions to the blockchain: A survey on proving schemes," *Computer Communications*, vol. 225, pp. 289–310, 2024.

[36] M. S. de Alencar and J. C. da Rocha, *Digital Communications*. Springer, 2025.

[37] Y. P. A. Sanjaya and M. A. Akhyar, "Blockchain and smart contract applications can be a support for msme supply chain finance based on sharia crowdfunding," *Blockchain Frontier Technology*, vol. 2, no. 1, pp. 44–49, 2022.

[38] K. Bohyer and T. Hayajneh, "Modernizing contracts across industries: a review of smart contract applications and the evolving legal landscape," *EAI Endorsed Transactions on Scalable Information Systems*, vol. 10, no. 5, pp. 1–11, 2023.

[39] M. Zrikem, I. Hasnaoui, and R. Elassali, "Vehicle-to-blockchain (v2b) communication: Integrating blockchain into v2x and iot for next-generation transportation systems," *Electronics*, vol. 12, no. 16, p. 3377, 2023.

[40] A. Rizky, R. W. Nugroho, W. Sejati, O. Sy *et al.*, "Optimizing blockchain digital signature security in driving innovation and sustainable infrastructure," *Blockchain Frontier Technology*, vol. 4, no. 2, pp. 183–192, 2025.

[41] R. Auer, B. Haslhofer, S. Kitzler, P. Saggese, and F. Victor, "The technology of decentralized finance (defi)," *Digital Finance*, vol. 6, no. 1, pp. 55–95, 2024.

[42] R. Singh, A. Gupta, and P. Mittal, "A systematic literature review on blockchain-based smart contracts: Platforms, applications, and challenges," *Distributed Ledger Technologies: Research and Practice*, vol. 5, no. 1, pp. 1–36, 2025.

[43] A. Gunawan, W. Hasyim, M. Putih, T. W. Wirjawan, I. A. Gopar, and S. Stephanie, "A comprehensive bibliometric study of digital leadership influence on technopreneurial success," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 7, no. 2, pp. 492–502, 2025.

[44] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur, and H.-N. Lee, "Systematic review of security vulnerabilities in ethereum blockchain smart contract," *Ieee Access*, vol. 10, pp. 6605–6621, 2022.

[45] H. Song, Y. Wei, Z. Qu, and W. Wang, "Unveiling decentralization: A comprehensive review of technologies, comparison, challenges in bitcoin, ethereum, and solana blockchain," in *2024 IEEE 6th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, vol. 6. IEEE, 2024, pp. 1896–1901.

[46] M. Bartoletti, L. Benetollo, M. Bugliesi, S. Crafa, G. Dal Sasso, R. Pettinau, A. Pinna, M. Piras, S. Rossi, S. Salis *et al.*, "Smart contract languages: A comparative analysis," *Future Generation Computer Systems*, vol. 164, p. 107563, 2025.

[47] M. M. Khan, F. S. Khan, M. Nadeem, T. H. Khan, S. Haider, and D. Daas, "Scalability and efficiency analysis of hyperledger fabric and private ethereum in smart contract execution," *Computers*, vol. 14, no. 4, p. 132, 2025.

[48] S. Andreina, T. Cloosters, L. Davi, J.-R. Giesen, M. Gutfleisch, G. Karame, A. Naiakshina, and H. Naji, "Defying the odds: Solana's unexpected resilience in spite of the security challenges faced by developers," in *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, 2024, pp. 4226–4240.

[49] M. Jin, R. Liu, and M. Monperrus, "On-chain analysis of smart contract dependency risks on ethereum," *arXiv preprint arXiv:2503.19548*, 2025.

[50] C. S. Götz, P. Karlsson, and I. Yitmen, "Exploring applicability, interoperability and integrability of blockchain-based digital twins for asset life cycle management," *Smart and Sustainable Built Environment*, vol. 11, no. 3, pp. 532–558, 2022.

[51] A. Bruel and R. Godina, "A smart contract architecture framework for successful industrial symbiosis applications using blockchain technology," *Sustainability*, vol. 15, no. 7, p. 5884, 2023.